Manuscript Submitted	Nov 11, 2020
Accepted	Nov 27, 2020
Published	Dec 21, 2020

An Enhanced Process of Digital Forensic to Support E-Crime Investigations Focusing on Evidence Handling in Malaysian Armed Forces

Pritheega Magalingam, Nurazean Maarop & Ganthan Narayana Samy
Advanced Informatics Department
Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
mpritheega.kl@utm.my, nurazean.kl@utm.my, ganthan.kl@utm.my

Mohd Hafzi Bin Marzuki
Malaysian Armed Forces Headquarters
Wisma Kementerian Pertahanan, Jalan Padang Tembak
Kuala Lumpur, Malaysia
mohdhafzi@mod.gov.my

Abstract

Digital Forensics Lab (DFL) in Malaysian Armed Forces (MAF) has been in operation since 2018, providing digital forensic services. The lab is in its maturing phase where the people and the process are still adjusting to the day-to-day operation. With the ease of the procured digital forensics tools, the analyst uses an explorative method to understand the tools' function, operations and has been following basic procedures and guideline given by Scientific Working Group on Digital Evidence (SWGDE). Thus, the purpose of this study is to propose an enhanced digital forensic process for DFL. The need for a comprehensive process is to ease the operation inside DFL whereby the current process can be organized into groups so that it is easily followed and implemented. To do so, a pilot study has been done through the literature review where numerous processes were studied, and their phases were compared to find the gap process. The digital forensics processes that were proposed do not consider any specific environment, where the authors gave a general process such as preparing, identify, analysis, preservation and reporting to be used. There is no proper evidence handling steps in each of the existing digital forensic phase followed by DFL. Two main elements, that are the legal and environmental factors should be taken into consideration when proposing a process. To gather more data, the mix method was chosen where qualitative data (from the interview, observation and documentary analysis were performed) and quantitative data (from questionnaires) were collected. Analysis of the data collected aided in the formation of the newly enhanced digital forensic process for the DFL. The enhanced process benefits the personnel in DFL to follow the digital forensic steps and use it as the main reference in their daily operation. The enhanced process also can be referred by any government or private sectors that have a dedicated digital forensic laboratory on their own. This is because even though the enhanced process is developed based on the MAF management requirement, the steps of each phase can be used and adapted to other agencies as well. The process suits the daily operation in the army environment; therefore, the proposed process is expected to be practical, precise and easily followed by the current personnel and novices.

***Keywords*:** *Digital Forensic, Evidence Handling, Digital Evidence, Process*

1. Introduction

The need for a comprehensive yet workable Digital Forensic process is to ease the operation inside DFL. Due to the rapid job transfers of personnel through inter departments in MAF, there are hardly

or few permanent staffs that remain to conduct the digital forensic process. This research proposes a comprehensive digital forensic evidence handling process that will be easy for the permanent and the recently transferred staff to quickly understand and adapt to the practice in a digital forensic lab.

Apart from not having a standard process on handling digital evidence, without proper documentation also will cause the evidence produced not be admissible in the court. The reason is, when a case is tendered to the court, it might take a long duration between the investigation stage and a trial stage, where without proper documentation, evidence can be considered as weak. Since digital forensics is a relatively new discipline in Malaysian Armed Forces, there is always room for error that might jeopardize the integrity of evidence, for which the cause of not having a comprehensive process to follow. In another note, one part of handling digital evidence is preservation. The data contained in digital evidence are volatile (Halim et al.) and preserving the evidence is vital to avoid any loss of a significant piece of information that might serve as the biggest clue to prosecute a perpetrator. The process in handling digital evidence, documenting important facts of the collected evidence, and preserving are essential components in making sure that evidence is admissible to the court.

Thus, for the evidence to be admissible, it must be reliable (Parkavi and Divya, 2020, Antwi-Boasiako and Venter, 2017, Horsman, 2019). Reliable in this context means the credibility of any source presented that is being used as evidence.

Based on the interview with Malaysian Armed Forces' personnel, the analysts in DFL handle and analyze digital evidence by following a basic guideline and their understanding from training. The lack of proper digital evidence handling process to maintain the credibility of the evidence is the main problem faced by the Malaysian Armed Forces for which MAF does not have a workable process. This motivates into the development of a comprehensive yet workable digital forensics process. Past digital forensic processes that were proposed since 2001 were studied.

Different organizations adopt different process when dealing with digital evidence that based on the suitability of the process's components to their daily operation. The first computer forensic investigative process with common phases that includes acquisition, identification, evaluation and admission was introduced by M.Pollit (Pollitt, 1995). Years later, in 2001, in the 1st Digital Forensics Research Workshop (DFRWS). Yusoff et al. (Yusoff et al., 2011) proposed a general-purpose digital forensics investigation process that comprises of 6 phases with three new phases that are preservation, analysis and presentation. Even though analysis and presentation correspond to evaluation and admission steps of the previous model, preservation is a new step introduced to make sure the evidence is not tampered and to maintain its originality. Preservation in another way that sustains the rules of evidence and its admissibility.

In 2002, Reith et al. proposed Abstract Digital Forensic Model with 9 phases. The three additional phases that were embedded in the earlier model in (Pollitt, 1995) are preparation, approach strategy, and returning evidence. In the preparation phase, activities such as tools preparation, identifying the techniques to be used, and getting management support were the initial tasks done. Approach strategy has been introduced to maximise the acquisition of untouched evidence and at the same time, minimising any negative impact on the victims and the people around them. To ensure that the evidence is returned safely to the intended recipient or proper disposal of the evidence, the phase returning evidence has been introduced. Thereafter, an event-based approach with 5 phases was introduced by Carrier et al. (Carrier and Spafford, 2004) in 2003 where the process is initiated with a phase that requires the physical and operational infrastructure to be ready to support any related future investigation. In this readiness phase, the equipment prepared must be ready, and the accountable analysts must have the appropriate skills of using it effectively. They focused on two investigations; digital crime and physical crime investigations. Their proposed digital crime scene investigation is similar to physical crime scene investigation with the exception that it is focusing on digital evidence in a digital environment but the detailed evidence handling process has not been clearly stated. In 2004, Carrier et al. (Carrier and Spafford, 2004) made changes to their model, removed two phases that are physical crime and digital crime investigation phase and replaced it with a traceback and dynamite phase. In the traceback phase, the analyst should have the ability to trace back the devices or computer being used by the perpetrator to commit the crime. It will include tracking down the source of crime scene, which consists of devices and location. During this phase, obtaining approval to perform an investigation and to gain crucial access to information is essential. Next in the dynamite

phase, extracted information need to be laid out and documented to construct possible events that might occur and to identify the perpetrator.

Meanwhile, Ciardhuain (Ciardhuáin, 2004) has proposed a process that covers all the essential steps of any given digital evidence investigation process and the process also provides a basis for the development of techniques and tools to support the work of the digital forensic analyst. Beebe et al. (Beebe and Clark, 2005) introduce a two-tier process where each phase in the first-tier requires a sub-phase OBSP (Objectives-Based Sub-Phase) for the proposed process to complete. OBSP consists of mini steps to be carried out for each phase. The mini steps are example layers of abstraction instead of detailed evidence handling steps. Kohn, et al. (Köhn et al., 2006) aims to propose an adaptable framework that only consists of three stages which are the preparation, investigation and presentation stage. The unique case for this is where it incorporates legal base as a foundation for the proposed framework by having an understanding of legal requirements. CFFTPM (Rogers et al., 2006) process consists of 6 phases. In this process, the unique phase that differs from the rest of the proposed model or framework before this is the Triage phase, where the evidence that is vital to the investigation is processed first. By observing the process, it is found that the process is much suitable for cases that deal with internet artefacts only.

FORZA-digital forensics investigation process was proposed by Leong (Ieong, 2006) where this process is unlike the other processes as there are three elements; roles, responsibilities of each role during an investigation and related standard procedure that has to be carried out by each role is incorporated in the process. It stated that the fundamentals are based on two principles; the IT Security principles which are integrity, confidentiality, and availability and the digital forensic principle that consists of reconnaissance, relevancy, and reliability. According to his paper, there are eight roles; case leader, legal advisor and prosecutor, system owner, security/system architect/auditor, digital forensics personnel (specialist, analyst, and administrator). These elements depend on each other to form a workable process. A study was also done on the work by Venter (Venter, 2006) that presents the process flows for cyber forensic training and operations. In each of the process flows the "Inspect & Prepare Scene", "Collect Evidence & Evidence Information", and "Debrief Scene & Record Seizure Information" elements were present. From the generic process elements, the author has proposed a few processes flows that involves Process Flow for Electronic Crime Scene, Process Flow for Seizing Desktop Computer Hard Disks, Process Flow for Seizing PDAs and Cell Phones and Process Flow for Seizing CD/DVD/STIFFY/FLASH/OTHER.

Kent et al. (Kent et al., 2006) proposed four phases for digital forensic process that includes collection, examination, analysis and reporting phase. In addition to the phase, the authors have shown how the evidence transforms from media to evidence that will be useful for the prosecutions. In 2007, a common process model for incident response and computer forensics was introduced by (Freiling and Schwittay, 2007) consist of three phases, that include Pre-Analysis, Analysis, and Post-Analysis. The Pre-Analysis phase is the step taken to identify incidents. The analysis phase is to analyse the incident by investigating what had happened, how the chronological events may affect the analysis, etc. The Post-Analysis, on the other hand, will document all the activities and steps taken during the previous phases and it is done in written report form. On the other hand, in 2008 (Khatir et al., 2008) a two-dimensional evidence reliability amplification process model was proposed. The model has a total of five main phases and 16 sub-phases that are tabulated to match with four categories of activities namely computer tools utilization, case management and team setup, preservation and authenticity and documentation respectively. In 2011, a systematic digital forensic investigation model was introduced by Agarwal et al. (Agarwal et al., 2011). This process incorporates 11 phases starting from preparation to the result phase. Apart from the usual phases seen in the previous process, starting from the third phase of this process that is from the documentation of scene to the evidence examination, another new element is incorporated in the process to capture the timeline according to the country's digital forensic law.

Even though many processes existed, none fit to the operation in DFL, for which this research attempts to gain information through survey and questionnaire that will lead to the development of an enhanced process for the Malaysian Armed Forces. Through the newly developed process, the upper management will understand that there is a process that is needed to be followed by the analyst and the time for analysis is time-consuming. The analyst should not be given a time frame to finish the

analysis, but instead, they should be allowed to work more on the digital evidence for the more comprehensive result while maintaining the integrity of the evidence. Through the use of the enhanced process, it is also expected to improve the operations in the laboratory and minimize error or inconsistencies when it comes to processing and handling digital evidence.

2. Literature Review

2.1 Previous Work in Malaysia and Gap Analysis

Digital forensic investigation models that were built based on the Malaysian investigation process were analyzed and the commonly shared processes are identified through a mapping process. It is found that three distinct phases have been highlighted in the former studies (Yusoff et al., 2011, Perumal, 2009, Perumal and Norwawi, 2010, Selamat et al., 2008), that are the Proof and Defense phase, Disseminating the Case Phase, and Archive Storage phase. Based on these research, the digital forensics processes that were proposed do not consider any specific environment, where the authors gave a general process such as preparing, identify, analysis, preservation and reporting to be used. Further analysis was done and this research has compared the phases of each model or process proposed in the past (Rogers et al., 2006, Parkavi and Divya, 2020, Carrier and Spafford, 2004, Ieong, 2006, Köhn et al., 2006, Antwi-Boasiako and Venter, 2017, Agarwal et al., 2011, Horsman, 2019, Khatir et al., 2008) with the current digital investigation process contained in the MAF guideline. Around 21 phases were identified and the important phase mapping is shown as in Table 1.

Table 1: Comparison of Digital Forensic Phases in Different Models or Processes

No	Model/ Process Name	Phases																				
		1.Awareness	2. Prepare/Authorization/	3. Notification	4. Secure the Scene & Communication Shielding	5. Acquisition	6. Identify	7. Deployment	8. Traceback	9. Approach Strategy	10. Collect/Reconnaissance	11. Preserve	12. Document Records	13. Transport and Storage	14. Examination/Analysis/ Evaluate	15. Hypothesis	16. Presentation and Reporting	17. Proof and Defense	18. Return Evidence/Case closed	19. Archive Storage	20. Review	21. Role-Based Investigation
1	Computer Forensic Process (M.Pollitt, 1995)					/	/				/				/							
2	DFRWS Investigative Model (Yusoff, Ismail & Hassan, 2011)		/				/				/				/		/					
3	Abstract Model of the Digital Forensic Procedure (Reith, Carr & Gunsch, 2002)		/				/			/	/	/			/		/		/			
4	An Integrated Digital		/					/							/						/	

	Investigation Process (Carrier & Spafford, 2003)																				
5	An Extended Model of Cybercrime Investigation (Ciardhuain, 2004)	/	/	/			/				/			/	/	/	/	/	/		
6	Enhance Integrated Digital Investigation Process (Baryamureeba & Tushabe, 2004)		/					/	/						/					/	
7	Hierarchical, Objective-based Process (Beebe & Clark, 2004)	/					/				/				/		/		/		
8	Investigation Process (Kohn, Eloff, & Oliver, 2006)		/												/		/				
9	Computer Forensics Field Triage Process Model (K.Rogers, Goldman, Mislan, Wedge, & Debrota, 2006)		/								/				/						
10	The Four Step Forensic Process (Kent et al,2006)										/				/		/				
11	The FORZA Process																				/
12	Process Flows for Cyber Forensics Training and Operations (Venter,2006)		/								/		/								
13	A common Process Model for Incident Response and Computer Forensics (Freiling & Schwittay, 2007)		/												/		/				

14	The two dimensional Evidence Reliability Amplification Process Model (Freiling & Schwittay, 2007)		/								/				/		/		/			
15	The Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal, et,al.,2011)		/		/						/	/	/		/		/					
16	Mapping Process of Digital Forensic Investigation Process (2008) Siti Rahayu Selamat, Robiah Yusof, Shahrin Sahib		/								/	/			/		/		/	/		
17	Digital Forensic Model Based On Malaysian Investigation Process (2009) Sundresan Perumal		/				/				/			/	/		/	/				
18	Common Phases Of Computer Forensics Investigation Models (2011) Yunus Yusoff, Roslan Ismail and Zainuddin Hassan		/				/				/	/			/		/					
19	Malaysian Armed Forces Digital Forensic Process (Existing Phase)			/							/	/		/	/		/		/			

Some phases of the past work carry the same meaning or derived from four basic digital forensic steps. To avoid repetition, similar steps are grouped as one relevant phase. Some literature refers to phases as components/classes/steps. Hereafter this study refers to these as a phase. In the current digital forensic process followed in DFL, there are altogether 14 phases, but most of the phases fall

onto the same category. Thus, for this research, 14 phases are reduced to 7 phases that are Notification, Collection, Preservation, Storage, Analysis, Reporting and Case Closed (see Table 1).

This study also focuses on the number of phases that are considered essential to be employed for a workable digital forensic process. Kohn et al. (Köhn et al., 2006) prove that a process can be as simple as 3 steps but Ciardhuain (Ciardhuáin, 2004) requires 13 phases to develop a comprehensive process. Whether it is a simple or a complex, the process should be adaptable to the environment that the digital forensic works take place.

2.2 Factors that Influence the Development of Digital Forensic Process

It is observable that there have been many attempts to develop a digital forensic process. However, so far none have been universally accepted (Rodgers, 2020). Part of the reason for this may be because many of the process models were designed for a specific environment, such as law enforcement, and they, therefore, could not be readily applied in other environments such as incident response. Thus, apart from the digital forensic field is still considered at its infancy, legal factor, the multi-environment factor does contribute to the different number of phases.

The digital investigation process has been directed by technology and the available tools. This is because most of the proposed procedures are developed by tackling different technology embedded in the inspected tools. However, the researchers should know that technology changes often and new procedures should be developed to cater to this need. While creating a standard process, one should avoid redundancies of procedures due to technology changes so that the new proposed model can simplify the process, and to make sure that the evidence is concrete to be presented in the court of law. Another issue derived from the literature is, most of the existing model design does not show the information process flow, no attention has been paid on the fragile evidence (live data acquisition and static data acquisition) and also on the data acquisition process to be used in cybercrime investigation.

There are some influencing factors when a process is developed. Most of the factors are due to the environmental factors; people, skill, location, type of evidence, duration of a case, etc. that lead to customizing the process to suit their respective operation. Legal concern is one common contributor when choosing the appropriate phase for the proposed process. Table 2 below shows the basic influencing factors that are derived from past work (Pollitt, 1995, Ciardhuáin, 2004, Carrier and Spafford, 2004, Kent et al., 2006, Köhn et al., 2006, Rogers et al., 2006, Freiling and Schwittay, 2007, Karie et al., 2016, Reith et al., 2002, Baryamureeba and Tushabe, 2004, Stephenson, 2003).

Table 2: Influencing Factors while Developing the Digital Forensic Process

No	Digital Forensic Investigation Process	Influencing Factor	
		Category	Description
1.	Computer forensics: An approach to evidence in cyberspace (Pollitt, 1995)	Legal	To comply with the legal requirement in court and science.
2.	A Generic Framework for Digital Evidence Traceability (Karie et al., 2016)	Environmental	To have a generic process that can be applied for a digital system including network investigations.
3.	An examination of digital forensic models (Reith et al., 2002)	Environmental	To have a general process that can be applied to categorizing of incidents.
4.	An event-based digital forensic investigation framework (Carrier and Spafford, 2004)	Environmental	Based on the investigation process of the physical crime scene.
5.	A Comprehensive Approach to Digital Incident Investigation (Stephenson, 2003)	Environmental	To focus on the analysis process and merging events from multiple locations.

6.	The Enhanced Digital Investigation Process Model (Baryamureeba and Tushabe, 2004)	Environmental	To reconstruct the primary crime scene (the computer) and the secondary crime scene (the physical crime scene) concurrently to avoid inconsistencies.
7.	Extended Model of Cybercrime Investigations (Ciardhuáin, 2004)	Environmental	To have clear steps during the investigation while providing a foundation when developing techniques and tools to support analyst.
8.	Event-based Digital Forensic Investigation Framework (Carrier and Spafford, 2004)	Environmental	Based on the event's causes and its effects
9.	A Hierarchical, Objectives-based Framework for the Digital Investigations Process (Beebe and Clark, 2005)	Environmental	Enhance the process proposed by (Carrier and Spafford, 2004) by introducing the objective-based task.
10.	Guide to integrating forensic techniques into incident response (Kent et al., 2006)	Environmental	To make evidence usable for the use of law enforcement and internal organization usage.
11.	Framework for a Digital Forensic Investigation (Köhn et al., 2006)	Legal & Environmental	Merging existing process into three minimum stages that conform to legal requirements.
12.	Computer Forensics Field Triage Process Model (Rogers et al., 2006)	Environmental	To have a process that covers field or onsite investigation without bringing the original evidence back to the laboratory.
13.	A Common Process Model for Incident Response and Computer Forensics (Freiling and Schwittay, 2007)	Environmental	The process combines the concept of Incident Response and Computer Forensics by improving the overall process of the investigation while it aims to investigate computer security incidents.

Referring to the background of this study, Malaysian Armed Forces can benefit from a good enhanced process that is developed specifically by considering all the influential factors. Besides, the design of the enhanced process must be developed based on digital forensic operations in DFL. The main aim of the enhanced process is, it should be able to minimise any errors from the start process to the end process when handling the digital evidence.

3. Methodology

In this section, information on the research method which includes data collection and sample, measurement items followed by data analysis and discussion of results were provided.

3.1 Data Collection

Three key personnel from the Malaysian Armed Forces were interviewed respectively to obtain data for the purpose of this research. The key personnel that were chosen are based on their availability, decision makers and those who have experience in digital forensic operation. Secondly, two subject matter experts from the field were interviewed to gain their opinion and suggestion on this matter. Observation was done by tagging along with the laboratory team members to gain an understanding of how they conduct day to day operations. Documentary analysis that involves seeing and analysing

how the records are being maintained was conducted. The observation and documentary analysis were done by getting permission from the department leader.

With the knowledge obtained from the interviews, documentary analysis and observations, questionnaires were set to gain the personnel understanding towards the digital forensic current operations and the underlying problems. 30 personnel were chosen since that is the total number of the current officers in the division and all of them have the knowledge of Digital Forensic process. By using the Statistical Packages for the Social Sciences (SPSS) tool, the data was analysed automatically.

3.2 The Research Process

The research process involves 4 main phases namely Preliminary study, Pilot study, Findings, and Reporting.

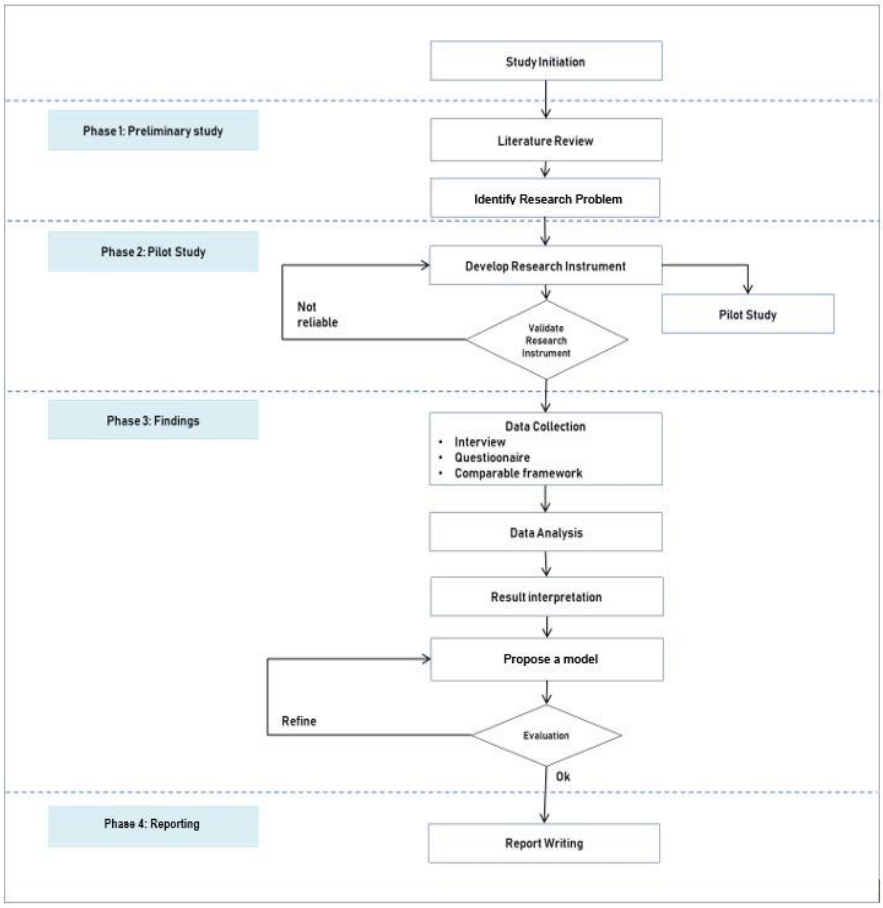


Figure 1: The Research Process

The preliminary study is the first phase of this research whereby it is highly involved in understanding the research problem. Through a thorough literature review, in-depth explanation of the study on how digital forensic and the discipline have evolved till today has been derived. A gap analysis was done on the previous works and it showed different phases that have been proposed or currently implemented in their respective environment. Following that, the most crucial stage that is the pilot study was conducted. This stage involves developing a research instrument to achieve the objective of the study. Validation of the research instrument helped to decide on the data collection method.

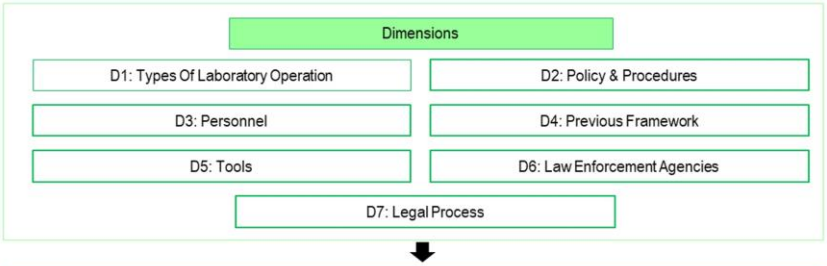
To obtain a sample of the study for the target population, purposive sampling technique was used. Purposive sampling technique is a method used to deliberate selection of particular units of interest.

The participants are selected based on their ability to provide the information needed to meet the purpose of the study. This technique was chosen based on the nature of the Cyber Defense Operation Centre (CDOC) division. Knowledgeable IT personnel in the digital forensics department is the targeted unit for this technique. CDOC is responsible for making sure that Malaysian Armed Forces premise is free from cyber threats. Apart from having CDOC as a security department that secures the perimeter, DFL is responsible in discovering and uncovering the act after a security breach occurs and also, a huge part in DFL is responsible in cybercrime investigation.

Qualitative data from the interview became the aid to analyze the existing problem and provided insights on how to generate the questionnaires for quantitative analysis. To analyse the qualitative data, input from the interview and observation was gathered, listed out, and categorised. Then, a series of questionnaires were generated and distributed to the Malaysian Armed Forces' personnel. The data from the questionnaires were analysed using Microsoft Excel and also SPSS. Through the analysis, a new model for the use of DFL will be proposed. Digital Forensic experts who are directly involved in the Digital Forensic Operations and Management later evaluates the proposed process and the results are recorded. The last part involves documentation and research paper writing.

4. Experiment

There are 7 main dimensions taken into consideration when developing the enhanced digital forensic process for MAF. The dimensions are Types of Laboratory Operation, Policy and Procedures, Personnel, Previous Framework, Tools, Law Enforcement Agencies and Legal Process. These dimensions also become the basis to identify the relevance of a certain process in each digital forensic phase. The Figure below shows the dimension mapping.



Questionnaire Section and Dimensions

Questionnaire Section	Dimensions
Section A: Demographic Profile	D1,D3
Section B: Involvement Towards The Operation in DFL	D3,
Section C: Awareness	D2,D3,D4
Section D: Digital Forensics Phases	All Dimensions
Section E: Digital Evidence Handling	All Dimensions
Section F: Components Of An Enhanced Process	All Dimensions
Section G: Impact	D3

Figure 2: The Dimension Mapping to Questionnaire Section

Demographic is defined as statistical data about the characteristic of a population such as age, gender and income of the people within the population. Target population within MAF is amount to 30 respondents where majority of them has working experience from 5 to 12 years in the field of digital forensics. Their insights are often sought when it comes to national defence and most of them are familiar towards the operations in DFL. 80% of the respondents strongly agree that Identify, Collect, Analyse, and Reporting are the basic phases in digital forensics. 87% of the respondents acknowledge that basics steps in digital forensics do exist, but another 13% disagree or unsure upon the basic phases.

Through the analysis, it is found that the current digital forensic process or the workflow in the workplace is developed by the personnel in DFL. To them, the current workflow that they have is the simplest form for them to follow since the laboratory is still new, and the personnel is trying to adapt to the discipline. The awareness is important among the personnel to understand the drawback and the risk of the current workflow and the need for the enhanced process. Most of the risk occurs when there is no proper digital evidence handling procedure at every phase. However, analysis shows that only 13.3% of the respondents have the initiative to betterment themselves in updating knowledge in handling digital evidence and 96.7% of them understands that evidence will not be admissible in the court of law without proper handling method.

The basic digital forensic phases are identify, collect, analyze and reporting. While analyzing the basic phases knowledge of the respondents, it is found that 66.67% of the respondents feel that the current workflow is not sufficient and need some additional steps, especially for evidence handling. The respondents also feel that there is a need to have a standardized process that suits DFL's current environment and could be used by other laboratories in the same environment or practice. Based on these statistics, this study proposed new components that start with a request for digital forensic service, consent from the supervisor, identification, assign a case, data collection, storage, analysis, reporting and end with closing the case. The proposed phases are accepted or agreed by the higher officials and marked as highly important by the respondents to be part of the newly enhanced process.

The impact analysis shows that the respondents are ready to implement the enhanced process in their department as they feel confident to become an expert witness as the through the proposed components, the data will be stored in a trusted way and it will maintain the chain of custody while conducting the digital forensic process. This will also make the operations in DFL runs smoothly and assist as a proper guideline in daily operation in DFL. With enhanced process implemented within the department, the department may see a positive impact, especially on how evidence is managed. Since the enhanced process will cover all the necessary steps, new or senior personnel can refer to it with no hassle since the new process will be a straightforward process, comprehensive yet understandable.

5. Proposed Enhanced Digital Forensic Process

The aim in handling digital evidence in a proper manner is to ensure that the analysis done onto the evidence is reliable and that the evidence is admissible in the court of law. It is done by making sure that the process from the first time the evidence was seized, the evidence was transferred, transported, storage and the analysis process always follow a proper chain of custody and ensuring that the evidence is not tempered by making sure that no possible alteration happened due to cross-contamination. Due to that, through this research, a few recommendations are listed down in Table 3 below, acting as a checklist and a guide for DFL since they do not have this kind of guide in a written form.

Table 3: Components of an Enhanced Process

GUIDELINE FOR EVIDENCE HANDLING	
(A)	TO DO BEFORE GOING TO RAID
	▪ Prepare the tools to before going to RAID.
	▪ Test the tools and keep a record of testing.
	▪ Bring a running case number so that the evidence can be labelled straight away at the crime scene.
(B)	TO DO FOR EVIDENCE (RAID/AT THE COUNTER)
	▪ Label the evidence
	▪ Photograph the crime scene
	▪ Photograph the evidence with the label
	▪ Photograph connections to the device (i.e. computers, wireless, firewall, servers, etc.)
	▪ Disconnect the internet connection etc. (especially on the mobile phone) securely
	▪ Document the findings
	▪ Seal the evidence
	▪ Fill in the description of the evidence in the Evidence Form
	▪ Make sure that the owner of the device has a copy of the Evidence Form
	▪ Fill in the Chain of Custody Form
(C)	TRANSPORTATION
	▪ Make sure that the evidence is not left unattended
	▪ For volatile/sensitive items – bubble wrap it to absorb shock
(D)	STORAGE
	▪ Inspect the evidence (i.e is labelled and sealed) before storing in evidence secure room
	▪ The evidence secure room cannot be accessed by unauthorized personnel
	▪ The chain of custody form is signed when taking the evidence to and from the evidence secure room
	▪ The evidence secure room's condition is proper for storing digital evidence- the temperature is set to dry, 25 degrees Celcius.
(E)	ANALYSIS
	▪ The analyst must ensure that no cross-contamination could ever occur to the evidence
	▪ The evidence is write-blocked before conducting any process onto the evidence
	▪ Do not do direct investigation onto the evidence – create working copies
	▪ The analysis is done based on best practices and type of evidence
	▪ Evidence must be in good condition and sealed before storing and after use
(F)	REPORTING
	▪ Produce report by considering the evidence route
	▪ Make sure to attach all the supporting documents
	▪ Prepare for expert testimony
(G)	CLOSE THE CASE

On top of that, to further explain the guideline in Table 3 above, a new enhanced Digital Forensic process to support e-crime investigations focusing on evidence handling is proposed as shown in Figure 3. It is a detailed process that focuses on the process and evidence handling so that through this detailed process, no steps are left out, and it is comprehensive enough to fit in the DFL operations.

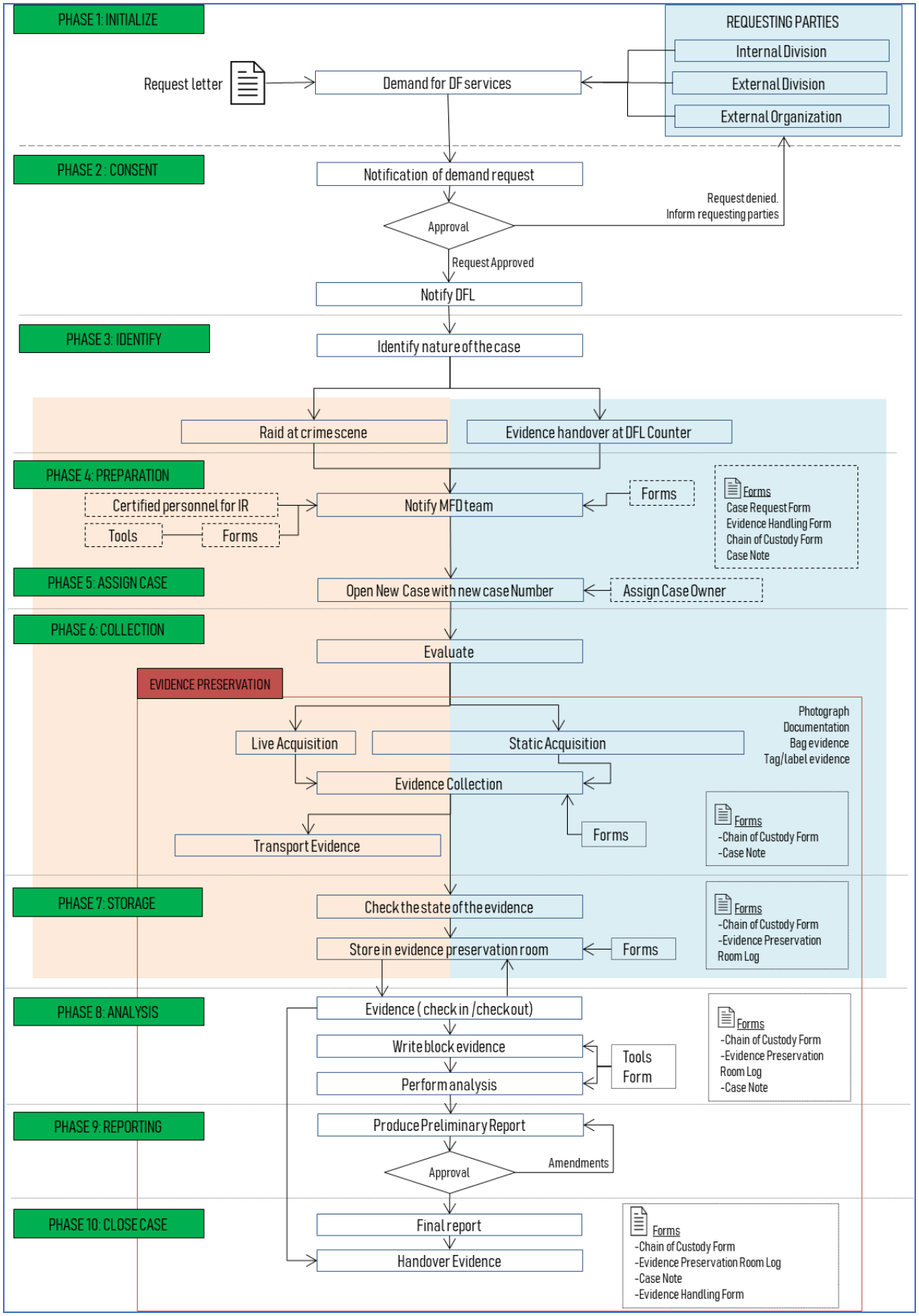


Figure 3: Enhanced Digital Forensic Process for Digital Forensic Laboratory, MAF

5.1 Details of the Enhanced Process

The enhanced process consists of 10 phases. The purpose of each phase is tabulated in the table below.

Table 3: Explanation on the Phases

Phase No	Phase Name	Explanation
1	Initialize	DFL receives a request for digital forensics analysis on a particular e-crime case
2	Consent	The request will go through the approval from the MAF Higher Official (decision maker)
3	Identify	If the request is approved, the appointed personnel from DFL will identify the nature of the case to decide on the raid at the e-crime scene and the analysis that is going to be conducted.
4	Preparation	The IR team from the DFL will prepare either for the raid for which they will bring the related tools and forms. In the case, if the evidence has been captured from the crime scene, the evidence will be received at the counter and the personnel will prepare the handover form.
5	Assign Case	Each case will get a running number and will have a person in charge (PIC) appointed for that case.
6	Collection	The PIC will evaluate the types and condition of the digital evidence and determine whether there is a need for live acquisition. The static acquisition can be made for both RAID and evidence received at the counter. Evidence preservation part is started from this phase.
7	Storage	Evidence is stored in the Evidence Preservation/Secure Room.
8	Analysis	Evidence is analyzed and the findings are documented.
9	Reporting	The report is made onto the results from findings
10	Close Case	The case is closed when the requestor signs off the case.

Evidence preservation happened from the sixth phase to the tenth phase. This is where evidence should be handled properly. In order to come out with the enhanced process design, the phases are the first thing that is taken into consideration. The work done by (Perumal and Norwawi, 2010) is taken as reference and is adapted in the new enhanced process. This is because the work done has two important attributes, that are the static acquisition and live acquisition. Both static acquisition and live acquisition is a crucial aspect that is needed to be considered when acquiring data. The steps for RAID are derived from Electronic Crime Scene Investigation: A Guide for First Responders (Investigation, 2001) and is also referred during when handling digital evidence at Evidence Preservation part proposed in Figure 3.

5.2 Comparison between the Current Workflow and the Newly Proposed Digital Forensic Process

Here we highlight the comparison of the current workflow of DFL, MAF and the enhanced process in Figure 3. One of the main differences between the current workflow (**A)** and the enhanced process (**B**); hereafter it is called as **A** and **B** respectively is that **B** is organized by 10 phases whereas **A** is only a series of process. **B** has compiled some of the information in **A** into groups in the phases. **B** also emphasizes on where evidence preservation must take place. The evidence preservation that is embedded in the evidence handling process is proposed from phase 6 to phase 10. **B** also takes into consideration of the process that happens during RAID (orange area) and during evidence handover at the lab (blue area) as per illustrated in Figure 3. **B** also highlights the necessary inputs of the forms

into the process because those forms are mandatory to be filled in, and it is important for auditing purposes.

6. Testing and Evaluating the Enhanced Process

The enhanced process, as in Figure 3 are presented to the personnel in DFL as part of the objective of this research. In order to test out the enhanced process, a discussion was done with a subject matter to validate the process. The subject matter experts (SME) including Mejar Nazaruddin bin Ahmad and his team's feedback upon the matter was very valuable. Based on the qualitative analysis, the record shows the enhanced process seems to be straightforward and can be easily executed by new or old employees. The further validation process is done with the other respondents by presenting the questionnaire data as well as the new proposed process. During the discussion, the respondents suggested that a walkthrough demo should be done to test the process. After the walkthrough, the respondents were satisfied to implement that in their working environment.

7. Conclusion and Future Recommendation

The main contribution of this work will benefit the personnel in Digital Forensics Laboratory (DFL) where upon research it is found that the laboratory needs a comprehensive process that they can use for their daily operation to improve the digital evidence handling. The enhanced process can be referred by any government or private sectors that have a dedicated laboratory on their own. This is because even though the enhanced process is developed based on the DFL management requirement, the phases and the process of each phase can be used and adapted by other agencies as well. The enhanced process can improve the e-crime investigation operation in the laboratory plus minimising error when it comes to processing and handling digital evidence.

In future, a comprehensive effectiveness testing of the proposed enhanced process is suggested for DFL. The process can be further expanded by having tools incorporated into the process and guideline can be build based on the different type of tools for various e-crimes.

Acknowledgement

The authors would like to thank the Ministry of Education, Government of Malaysia and Research Management Centre, Universiti Teknologi Malaysia for supporting this work through the Tier-2 Grant, vote number 16J48.

References

AGARWAL, A., GUPTA, M., GUPTA, S. & GUPTA, S. C. 2011. Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS),* 5**,** 118-131.

ANTWI-BOASIAKO, A. & VENTER, H. A model for digital evidence admissibility assessment. IFIP International Conference on Digital Forensics, 2017. Springer, 23-38.

BARYAMUREEBA, V. & TUSHABE, F. 2004. The enhanced digital investigation process model. *Digital Investigation*.

BEEBE, N. L. & CLARK, J. G. 2005. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation,* 2**,** 147-167.

CARRIER, B. & SPAFFORD, E. 2004. An event-based digital forensic investigation framework. *Digital Investigation*.

CIARDHUÁIN, S. Ó. 2004. An extended model of cybercrime investigations. *International Journal of Digital Evidence,* 3**,** 1-22.

FREILING, F. C. & SCHWITTAY, B. 2007. A common process model for incident response and computer forensics. *IMF 2007: IT-Incident Management & IT-Forensics*.

HALIM, N. B. A., GINSIM, S. & BAHARUDDIN, S. K. B. CASE STUDIES: ADMISSIBILITY OF DIGITAL RECORDS AS LEGAL EVIDENCE IN MALAYSIA.

HORSMAN, G. 2019. Tool testing and reliability issues in the field of digital forensics. *Digital Investigation,* 28**,** 163-175.

IEONG, R. S. 2006. FORZA–Digital forensics investigation framework that incorporate legal issues. *digital investigation,* 3**,** 29-36.

INVESTIGATION, N. I. O. J. T. W. G. F. E. C. S. 2001. *Electronic crime scene investigation: A guide for first responders*, US Department of Justice, Office of Justice Programs, National Institute of Justice.

KARIE, N., KEBANDE, V. & VENTER, H. A generic framework for digital evidence traceability. European Conference on Cyber Warfare and Security, 2016. Academic Conferences International Limited, 361.

KENT, K., CHEVALIER, S., GRANCE, T. & DANG, H. 2006. Guide to integrating forensic techniques into incident response. *NIST Special Publication,* 10**,** 800-86.

KHATIR, M., HEJAZI, S. M. & SNEIDERS, E. Two-dimensional evidence reliability amplification process model for digital forensics. 2008 Third International Annual Workshop on Digital Forensics and Incident Analysis, 2008. IEEE, 21-29.

KÖHN, M., OLIVIER, M. S. & ELOFF, J. H. Framework for a Digital Forensic Investigation. ISSA, 2006. Citeseer, 1-7.

PARKAVI, R. & DIVYA, K. 2020. Digital Crime Evidence. *Critical Concepts, Standards, and Techniques in Cyber Forensics.* IGI Global.

PERUMAL, S. 2009. Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security,* 9**,** 38-44.

PERUMAL, S. & NORWAWI, N. M. 2010. Integrated computer forensic investigation model based on Malaysian standards. *International Journal of Electronic Security and Digital Forensics,* 3**,** 108-119.

POLLITT, M. Computer forensics: An approach to evidence in cyberspace. Proceedings of the National Information Systems Security Conference, 1995. 487-491.

REITH, M., CARR, C. & GUNSCH, G. 2002. An examination of digital forensic models. *International Journal of Digital Evidence,* 1**,** 1-12.

RODGERS, K. D. 2020. *Required Elements for Constructing a Highly Adoptable and Adaptive Digital Forensic Model.* Capella University.

ROGERS, M. K., GOLDMAN, J., MISLAN, R., WEDGE, T. & DEBROTA, S. 2006. Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law,* 1**,** 2.

SELAMAT, S. R., YUSOF, R. & SAHIB, S. 2008. Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security,* 8**,** 163-169.

STEPHENSON, P. 2003. A comprehensive approach to digital incident investigation. *Information Security Technical Report,* 8**,** 42-54.

VENTER, J. 2006. Process flows for cyber forensic training and operations.

YUSOFF, Y., ISMAIL, R. & HASSAN, Z. 2011. Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology,* 3**,** 17-31.